Performance Work Statement (PWS)
Naval Facilities Engineering Systems Command (NAVFAC)
Risk Management Framework (RMF) Assess and Authorize/Cybersecurity Safety (CYBERSAFE)

1.0 Background

NAVFAC builds and maintains sustainable facilities, delivers utilities and services, and provides Navy expeditionary combat force capabilities. NAVFAC supports this mission through operational execution within six (6) Business Lines: Design and Construction, Environmental, Expeditionary, Public Works, Asset Management, and Contingency Engineering. NAVFAC's ability to realize its vision via the Business Lines is dependent on its ability to better capture, store, analyze, reengineer, and report on information and business processes it generates/collects within mission readiness. Enhancing data and information technology management, visualization, collaboration, warehousing, and cybersecurity efficiency and effectiveness will directly enhance the warfighter supply chain resulting in cost reductions and increased customer and leadership expectations.

NAVFAC Command Information Office (CIO) has been designated as the Functional Authorizing Official (FAO) and Functional Security Control Assessor (FSCA) for Facility Related Control Systems (FRCS) and must implement RMF/CYBERSAFE program requirements to allow for the determination of vulnerabilities, actions, and process changes required, and creation of correction action plans in order to bring both legacy and new systems into compliance with Department of Defense (DoD), Department of Navy (DoN), and RMF and CYBERSAFE mandates. The CIO is responsible for IT resource utilization, IT business process agility to meet emerging and evolving business and operational drivers, end user satisfaction, and overall cyber security to support an effective warfighter supply chain.

1.1 Objectives

The objective of this PWS is to establish performance requirements between the Government and the Contractor by outlining the scope of work to be performed to ensure successful delivery of services to the Government. Accordingly, contract support services are required to execute the tasks detailed in this PWS, deliver high-value business solutions and capabilities to employees, partners, and customers, while achieving maximum cost effectiveness, high customer satisfaction, and compliance with applicable federal laws and regulations to enable NAVFAC CIO mission effectiveness and readiness.

The Contractor shall provide cost-effective, efficient, and innovative solutions for meeting the mission and program objectives of NAVFAC. Overarching objectives include:

a. strengthening the CYBERSAFE program for execution of its six phases while ensuring alignment to NAVFAC's Systems Engineering Technical Review (SETR) and RMF processes.

b. obtaining expertise from industry to support NAVFAC's objectives to solve difficult technology issues that exist with securing FRCS.

c. managing, securing, and sustaining industrial control systems critical to the warfighter mission through the implementation of security controls that mitigate risks with Navy FRCS.

d. streamlining the current RMF process to foster quicker security control implementations, more accurate risk determinations, and more complete authorization determinations.

e. automating the RMF process, standardizing security control implementation and assessment techniques for Operational Technology/Industrial Control Systems (OT/ICS).

2.0 Performance Requirements

The Contractor shall perform the work and provide the CIO support in the following task areas. The Contractor shall provide the requisite program knowledge and the analytical, technical, engineering expertise and consultative services necessary to effectively and efficiently perform the work described in this PWS.

The requirements described Sections 2.1 through 2.3 of the PWS are "Core Services" and correspond with CLINx100.

2.1 Command Information Officer (CIO) Program Management Support

All programs within this PWS shall require the Contractor to work closely with the Government program manager and support the needs of the program at the sponsor level and within the general and/or tailored Department of Navy Systems Engineering Technical Review process. The Contractor shall coordinate program status meetings and technical reviews, prepare budget drills, develop agenda items, attend high level meetings, generate minutes, and track action items. The Contractor shall research policies, doctrine, tactics, and procedures at the Federal, State, and Local level and provide analysis. Program support shall require significant coordination and interface with various DOD and non-DOD activities located in and out of CONUS.

The Contractor shall document, for review and approval of the Government, its approach to managing this task order in a Program Management Plan (PMP) and how it will ensure quality in a Contractor Quality Control Plan (QCP).

The Contractor's Program/Project Management support includes the following specific responsibilities:

1. Scheduling, coordinating, and hosting a project kick-off meeting within 10 days after contract award at the location approved by the Government.
2. Establishing processes to govern the other tasks in this document, including risk management, schedule management, cost management, and quality management.
3. Delivering weekly and monthly status reports that provide programmatic and financial updates to include:
    a. Status of current and planned tasks and subtasks
    b. Planned schedule overlaid with actual schedules for each task
    c. Project Organization
    d. Project Transition Processes and Schedule
    e. Work Breakdown Structure (WBS)
    f. Overall Organizational Structure
    g. Task dependencies and interrelationships
    h. Staffing Plan
    i. Updated Deliverable Schedule
    j. Contractor Travel Information
    k. Prepare and conduct routine project review meetings
    l. Manage schedules, milestones and cost
    m. Establish and implement risk and issue management process
    n. Review schedule, milestones, budget, risks, and deliverables
    o. Develop concise, creative, and effective messages and materials both online and print for the public, media, and internal use.

4. Provide supporting IT/OT strategy and planning by integrating business and IT/OT processes, allowing for continuous evaluations and adjustments in response to new opportunities and changing operational conditions:
   a. Strategy on IT/OT transformation to reshape IT/OT operations and organizations to better support NAVFAC's mission
   b. Strategy on IT/OT strengths and risks across a wide array of IT disciplines
   c. Supporting NAVFAC IT value management by formalizing the tools, processes and metrics needed to drive greater value from IT/OT portfolio investments
   d. Conduct Business process mapping and reengineering as directed
   e. Provide analytical information papers on new technology insertion and potential impacts to NAVFAC operations
5. The Contractor shall track logistics of teams/individuals traveling in support of this task order to ensure proper JPAS visit requests and training is completed in alignment with the 1650 assessment team and schedules.

2.1.1 Enterprise Architecture (EA) Support

The Contractor shall provide enterprise architecture support to the command Enterprise Architect in the effort to document current state architectures, map architecture to modernization efforts as needed, analyze and ensure command/application architecture products meet Department of Defense architecture standards and frameworks as applicable, such as but not limited to Defense in depth functional implementation architecture (DFIA) and Department of Defense Architectural Framework (DODAF). Identify best practices and communications between services internal to NAVFAC and between NAVFAC and external interfaces and data sources. The Contractor shall encompass the architecture outputs to integrate into the current architecture roadmap and continue to build out NAVFAC's internal EA repository to enable analysis and solution integration.

2.1.2 Data Management Strategy Support

The Contractor shall develop Enterprise Data warehousing concepts, plans, and execution operating procedures that will integrate with the current NAVFAC Enterprise Data Warehouse. The strategy will encompass but is not limited to; Data source definition and target mappings; data extraction and transformation concepts; data error handling and recovery methods; data quality assurance standards; data governance structures influenced by higher DoD organizations and tailored to meet NAVFAC requirements; data elements and meta data dictionaries; data models and structures for both logical and physical data. Foundational to this strategy is the data analytics construct. The Contractor shall synthesize the data management strategy with the data analytics effort to ensure valid data points are produced to support robust decision making.

2.1.3 Automation Support

The Contractor shall develop and implement automation into CIO processes, including RMF. The RMF process can be a tedious process with many mundane tasks required to complete the RMF package and manage risk at an enterprise level. When requested by the NAVFAC Echelon II Chief Information Security Officer (CISO), FSCA, or FAO CSA.

2.2 Cybersecurity Safety (CYBERSAFE) Program Support

The Contractor shall provide expertise to ensure CYBERSAFE controls and management principles are incorporated, tested, and audited in system development outputs. The Contractor shall ensure the six CYBERSAFE phases (1: Assign Grade, 2: Identify Controls, 3: Implement Controls, 4: Certify, 5: Operate, 6: Monitor) are aligned to and are a foundational component of, the Department of Navy and NAVFAC Systems Engineering Technical Review (SETR) and the Risk Management Framework (RMF) process. The Contractor shall provide SME support to Echelon II CYBERSAFE Technical Warrant Holder (TWH) in executing CYBERSAFE warranting activities. The Contractor shall provide assistance and technical analysis to system owners and Information System Security Managers (ISSMs) in the execution of CYBERSAFE Certification Assessments. The Contractor shall build a repeatable and iterative program management reporting framework to incorporate CYBERSAFE into leadership briefings such as resources and requirements review boards and systems and test readiness reviews.

The Contractor shall serve as CYBERSAFE support project management lead, coordinate Criticality Analysis (CA) execution and ensure CYBERSAFE grading activities are executed and tracked appropriately. The Contractor shall provide development, management and oversight of the CYBERSAFE program office's policy and procedures, in support of government objectives and maturing of the program. The Contractor shall track working timelines and provide updates at regularly scheduled meetings.

The Contractor shall work in partnership with the NAVFAC Cyber Security and Technology engineering communities of practice to ensure CYBERSAFE principles and protocols are addressed and tracked via the internal NAVFAC CYBERSAFE tracker.

2.2.1 Systems Engineering Technical Review (SETR) Support

The Contractor shall support development of the NAVFAC SETR Instruction and execute the SETR process NAVFAC systems. The Contractor shall support SETR-related meetings and capture updates and lessons learned from the pilots to complete development of a final instruction.

2.2.2 Fleet Experimentation (FLEX) Support

The Contractor shall provide assistance in logistics, planning, and data calls for the execution of war games, such as FLEX or Trident Warrior, and develop briefing material as required or requested by CYBERSAFE Program Office (CSPO). The Contractor shall attend briefings in support of CSPO and create products necessary to support NAVFAC's involvement within various war games. The scope of this support includes:

- developing, participating, and evaluating Fleet Exercises
- participating in exercises to test and validate Fleet readiness and lethality as part of agency war game initiatives, inclusive of other Navy commands and joint services.
- analyzing cyber attack Tactics, Techniques, and Procedures (TTPs) during exercises and providing mitigation recommendations
- supporting vulnerability assessments through various techniques to validate response and recovery countermeasures

2.2.3 CYBERSAFE Technical Support

The Contractor shall assist CYBERSAFE Technical Director with the development of policies, procedures, and guidance on a technical approach to the CYBERSAFE program. The Contractor shall provide technical capabilities to assist with the development of custom mitigations to challenging technical requirements. The Contractor must be experienced with security control assessments to assist with determination on compliancy with CYBERAFE standards and procedures.

2.2.4 CYBERSAFE Grading Support

The Contractor shall support efforts in respect to Cyber Commissioning (CyCx) to identify task critical assets (TCA) in approved MILCON projects. The Contractor shall perform CYBERSAFE grading efforts of MILCON projects that are likely preliminary design authority (PDA) candidates.

The Contractor shall track the execution of NAVFAC's CYBERSAFE grading process, manage the NIPR/SIPR collaboration suites. Contractor shall execute correspondence with various Facilities Engineering Command (FEC) personnel to ensure timely responses aligned with CYBERSAFE processes and timelines per the NAVFAC CYBERSAFE Grading SOP in support of the CSPO.

2.2.5 Criticality Analysis (CA) Support (Travel Team)

The Contractor shall execute NAVFAC CYBERSAFE CA checklist while interviewing stakeholders and ensure required artifacts (HW/SW, network diagrams and other various documents in support of the CYBERSAFE Mission) are accurate. The Contractor shall assist in the development of such artifact and develop these artifacts where necessary. The Contractor shall execute the CYBERSAFE system and component grading process and ensure proper adjudication prior to onsite visit. The Contractor shall develop and present briefing materials to ensure all stakeholders are aware of how the CA process works. The Contractor shall train onsite personnel (which may include military or civilians at a site) on how to execute the NAVFAC CYBERSAFE CA, and act as the point of contact when sites require clarification or assistance.

2.2.6 Adversarial Assessment

The Contractor shall assist NAVFAC with completing adversarial assessment testing/penetration testing. The Contractor shall develop technical documentation detailing findings from penetration testing events and prepare briefing materials for CSPO. The Contractor shall assist NAVFAC with developing and executing adversarial (penetration) testing, develop recommended mitigation strategies and track such mitigations of findings.

2.3 Risk Management Framework (RMF) Support

The Contractor shall provide NAVFAC with FRCS Qualified Validator, FSCA Liaison, FAO Cyber Security Analyst, and automation support that follows the NAVFAC FRCS RMF Business Rules throughout the RMF for new and existing NAVFAC systems including, but not limited to the following use cases:

- Initial Assess and Authorize – Legacy System
- Initial Assess and Authorize – New System
- Renew Authorization – Existing Authorized System
- Decommission and Deauthorize

- Assess Only
- RDT&E Enclave Zone C and D
- Use Case III and IV System Baseline Changes

Each NAVFAC FRCS is different. These differences include, but are not limited to; number of components, location, accessibility, applications, and government developed code. FRCS Qualified Validator and FSCA Liaison levels of effort will fluctuate depending on the use case being supported and the complexity of the system.

2.3.1 FRCS Qualified Validator (FQV) Support

The Contractor shall provide NAVFAC CIO support in performing the duties of a Navy Qualified Validator (NQV) at each of the six steps of the RMF Process. In addition to the requirements established by the Navy Security Control Assessor (SCA), the Contractor must also meet the requirements to be certified per the NAVFAC CIO Memorandum on August 13, 2020, "Special Requirements for NAVFAC Facility Related Control System Qualified Validator."

The Contractor shall provide consultative support to the Information Systems Security Engineer (ISSE) and Information Systems Security Manager (ISSM) in the appropriate selection of security controls. Ensure required artifacts (HW/SW, network diagrams, other various documents) are accurate and develop\update these artifacts where necessary. Provide support and develop the Security Assessment Plan (SAP) based upon the required artifacts.

The Contractor shall complete the NAVFAC Validator Step 2 Checklist and support the ISSM in initiation of the System Security Plan in Enterprise Mission Assurance Support Service (eMASS.) The Contractor shall provide consultative support to the ISSE and ISSM in the documentation of security controls and development of the Information System Continuous Monitoring (ISCM) plan.

The Contractor shall provide SME consultative support to the ISSE and ISSM in implementation and testing of security controls during RMF Step 3. The Contactor supports the ISSM and ECH II Package Submitting Officer (PSO) in preparation and submission of a complete and accurate SAP at the beginning of RMF Step 4. The Contractor shall support the execution of the Security Assessment, RMF Step 4.

The Contractor shall conduct a complete security control validation and assessment of technical and nontechnical security features of a system or network to address known threats and vulnerabilities. The evaluation must consider and identify impacts as well as consideration of existing risk mitigation strategies.

The Contractor shall ensure traceability of all vulnerabilities from raw assessment results to the POA&M. Conducts required vulnerability analysis to support mitigation and residual risk determination; and supports the PM and ISSM in creating updates to the POA&M during RMF Step 4. The Contractor is responsible for initiating the Security Assessment Report (SAR) in RMF Step 4 and updating the SAR throughout the execution of RMF Step 4, based on the security control assessment results.

2.3.2 FSCA Liaison Support

To perform the Functional Security Control Assessor (FSCA) function in the most efficient manner, the FSCA may utilize a team of FSCA Liaisons to assist with FSCA responsibilities, where applicable. The FSCA Liaison will act as the FSCA's direct representative and will interface with the Program Manager/Information System Owner (PM/ISOs), ISSMs, ISSEs, Validators, PSOs, and Functional Authorizing Official (FAO) Cyber Security Analyst (CSA), as directed.

- The FSCA Liaison must be a risk assessment SME and provide support and assistance in the Assessment & Authorization (A&A) effort.
- The FSCA Liaison must also be a Navy Qualified Validator and a NAVFAC FQV.

FSCA Liaison-specific responsibilities include the following and the Contractor shall perform these approved FSCA Liaison RMF process steps:

- Provides consultative support to the ISSE and ISSM in the appropriate selection of security controls
- Supports the ISSM in initiation of the system Security Plan in eMASS as required.
- Provides consultative support to the ISSE and ISSM in the documentation of security controls.
- Provides SME consultative support to the Validator in creation of the SAP.
- Provides SME consultative support to the ISSE and ISSM in implementation and testing of security controls during RMF Step 3.
- Provides SME consultative support to the ISSE in initiating the Plan of Actions and Milestone (POA&M) during RMF Step 3.
- Provides SME consultative support to the Validator in execution of the Security Assessment of RMF Step 4.
- Accountable for the finalized and completed SAR Executive Summary.
- Supports the FAO and FAO CSA in making an authorization decision during RMF Step 5.

The Contractor shall assess approved technical and non-technical security features of a system or network to address known threats and vulnerabilities. The evaluation must consider and identify impacts as well as consideration of existing risk mitigation strategies.

The Contractor shall act as an independent and impartial assessor to determine and certify aggregate cybersecurity risk for recommendation to the SCA.

The Contractor shall provide initial concurrence on behalf of the FSCA for the SAP, ensuring all appropriate security controls will be assessed for compliance.

The Contactor shall provide quality assurance of an RMF SAP related to cybersecurity risk.

The Contractor shall develop the SAR with FSCA concurrence.

The Contractor shall guide and mentor Validators on the following:

- Understanding of the RMF risk assessment process
- Knowledge of implementation and applicability of Security controls
- Use of appropriate test procedures and tools
- Recommending mitigation measures for specific vulnerabilities
- Reviewing and concurring/non-concurring with Validator’s residual risk
- Traceability of test results to system components and the risk assessment, as reflected in the relevant RMF documentation
- Understanding of Cybersecurity policies and the effects of specific policies to the risk of a system
- Providing cybersecurity risk assessment technical assistance to the PSO to include ensuring triage reviews of packages are performed and documented for uniformity and completeness.

The Contractor shall support the ECHII/PSO in reporting metrics in support of Federal Information Security Management Act (FISMA), CyberScope reporting, and Cyber Resiliency reporting as required.

The Contractor shall provide guidance and assistance to sites managers and system owners to remediate or mitigate open/outstanding actions contained in POA&M for assigned systems and enclaves.

The Contractor shall provide eMASS expertise and lessons learned to the NAVFAC cybersecurity community.

The Contractor shall assist the ECH II CISO in the development of Vulnerability Remediation Asset Manager (VRAM) and follow-on vulnerability management system workflows and business processes.

The Contractor shall provide SME support to the ECH II CISO in creation and updates to cybersecurity policy and business process documents.

2.3.3 Functional Authorizing Official (FAO) Cyber Security Analyst (CSA) Support

To perform the FAO function in the most efficient manner, the FAO may utilize a team of FAO Cybersecurity Analysts (CSA) to assist with FAO responsibilities where applicable. The responsibilities of FAO CSAs include but are not limited to the following:

The Contractor shall perform the required FAO CSA RMF process steps on behalf of the FAO:

- Accountable to provide formal concurrence with the RMF Step 1 Information Categorization for submitted systems and enclaves.
- Accountable to support the ISSE in the tailoring of Security Controls during RMF Step 2.
- Provides SME consultative support to the PM and ISSM in creation of the ISCM strategy.
- Responsible to provide formal concurrence of Security Control selection and tailoring during RMF Step 2.
- Provides SME consultative support to the ISSE and ISSM in implementation and testing of security controls during RMF Step 3.
- Provides SME consultative support to the ISSE in initiating the POA&M during RMF Step 3.
- Provides SME support to the Validator in execution of the Security Assessment of RMF Step 4.
- Responsible to process the RMF Package with recommendation for AO signature during RMF Step 5.

The Contractor shall review and adjudicate system security categorization decisions through collaboration and ultimately by recommending approval of the Security Plan (SP).

The Contractor shall review final security control sets for DoD systems and provide approval recommendation to FAO.

The Contractor shall review the SP and system-level ISCM Strategy submitted by the PM/ISO and provide approval recommendation to FAO

The Contractor shall attend Checkpoints and provide initial approval or disapproval on behalf of the FAO (to include SP, ISCM adjudication).

The Contractor shall ensure RMF process steps are followed and adhered to by RMF stakeholders.

The Contractor shall establish and/or provide Subject Matter Expert (SME) guidance to RMF stakeholders on RMF processes and procedures

The Contractor shall ensure Authorization decisions are supported by sufficient documentation and accurate risk assessments.

The Contractor shall ensure authorization recommendations comply with higher level policy as defined by DoD/Navy policy.

The Contractor shall provide technical analysis of RMF artifacts to inform the authorization decision, in support of the FAO.

The Contractor shall support monitoring and tracking execution of POA&Ms for NAVFAC FRCS.

The Contractor shall provide SME support to the ECH II CISO in creation and updates to cybersecurity policy and business process documents.

2.4 Optional Requirements

The requirements described Section 2.4 of the PWS are "Optional Services" and correspond with CLINx200 and CLINx300.

The Government shall have the unilateral right to exercise options in whole or in part. Optional requirements will be funded at the time they are exercised.

For proposal purposes, include the CONUS and OCONUS labor rates for the corresponding Alliant labor categories/skill levels that will be used to fulfill the optional requirements for CLINx200 and CLINx300 described below. The Not-to-Exceed (NTE) value of the options for each year of performance are listed below:

Optional CLIN	Base Period NTE	Option Year 1 NTE	Option Year 2 NTE	Option Year 3 NTE	Option Year 4 NTE
CLIN x200	$3,800,000	$3,800,000	$3,800,000	$3,800,000	$3,800,000
CLIN x300	$2,000,000	$2,000,000	$2,000,000	$2,000,000	$2,000,000

2.4.1 Optional Project-Specific Support (CLINx200)

The Government reserves the unilateral right to exercise optional Project-Specific Support for RMF requirements that may arise under the scope of this PWS. It is anticipated that the Government will need support, on an optional basis, for the various scenarios as outlined in the table below.

At the time of exercising optional services the Government will definitize requirements in a Technical Direction Letter (TDL) that:

- Defines the duration, extent of support, and nature of work to be performed;
- Specifies the place(s) of performance and technical details about the project;
- Identifies the deliverables and associated due dates;
- Defines operating hours within which support is required;
- Identifies any travel requirements (if any);
- Specifies any special procedures or security clearance requirements.

The Contractor shall respond to the TDL in writing within seven (7) days, or as otherwise specified in the TDL, with a proposal showing the staffing plan to meet the Government's requirements.

TDLs may be exercised on a Firm Fixed Price or Time & Materials basis. TDLs may be issued on a severable or non-severable basis

Scenario Descriptions

In support of the following scenarios, the Contactor may be tasked with conducting, on an optional basis, unbiased, comprehensive assessments of the management, operational, and/or technical security controls and control enhancements employed within or inherited by an information technology (IT) system. The Contractor shall make and document determinations regarding the overall effectiveness of the controls, as defined in NIST 800-37 and IAW the RMF/CYBERSAFE requirements defined in this PWS.

Assessment and Authorization work will be accomplished using readily available approved tools. Program is responsible for providing Integrated Development Environment, (including code scan tools) for custom code (if any).

Scenario I	**Initial Assess and Authorize – Legacy System in Operation** - provide for software vulnerability analysis for legacy operational systems - provide model based systems engineering support - provide recommendations of architecture design and system upgrades to meet current cyber requirements - provide POAM oversight tracking - provide advice, make recommendations, produce technical artifacts and briefings - perform travel, if any, in support of assessment and authorization requirements
Scenario II	**Initial Assess and Authorize – Developmental System** - provide for software vulnerability analysis for developmental systems - provide model based systems engineering support - provide support for consulting/advisement on cyber security taskings, as necessary, to integrate security within the systems development lifecycle process, inclusive of consulting on and making recommendations regarding implementation and/or sustainment of operational systems - provide POAM oversight tracking - provide advice, make recommendations, produce technical artifacts and briefings - perform travel, if any, in support of assessment and authorization requirements and cyber-related taskings
Scenario III	**Renew Authorization – Existing System Already Authorized** - provide software vulnerability analysis using readily available tools, including freeware - provide model based systems engineering support - provide POAM oversight tracking - provide advice, make authorization recommendations, produce technical artifacts and briefings - perform travel, if any, in support of authorization and cyber-related taskings
Scenario IV	**RDT&E Enclave Zone C and D** - as definitized in TDLs, provide vulnerability analysis for applicable RDT&E Zone C& D Enclaves

	- perform travel, if any, in support of RDT&E Enclave Zone C&D
Scenario V	**Use Case III Memorandum for the Record (MFR) System Baseline Change** - as definitized in TDLs, provide vulnerability analysis for changes to system baseline. - Where necessary provide support for changes that must go through a full reauthorization - provide POAM oversight tracking - provide advice, make authorization recommendations, produce technical artifacts and briefings - perform travel, if any, in support of RDT&E Enclave Zone C&D Notes: FSCA approves the workflow FAO signs the Authorization Decision Document in eMASS

2.4.2 Optional Surge Support (CLINx300)

The Government reserves the unilateral right to exercise Optional Surge to support unforeseen, ad hoc requirements or unplanned increases in workload that may arise under the scope of this PWS. Optional surge will be invoked at the Government's discretion through a written modification issued by the GSA Contracting Officer.

As an agency of the DoD, NAVFAC must respond to real-world changes, whether it is a new reform initiative, top-down policies and mandates, or even national security interests and immediate threats. It is essential that NAVFAC has the resources and means to support evolving threats. This includes short-term (180 calendar days) response to implement directives, support to cybersecurity-related events, and surge to support complex upgrades. The Contractor shall use industry best practices and subject matter expertise to execute additional, as–needed, related projects. Surge support shall include, but is not limited to, the following:

- Additional resources to support RMF/CYBERSAFE and A&A activities and requirements defined in the PWS Sections 2.1, 2.2, 2.3
- Rapid capabilities that mitigate or resolve major IT issues, cybersecurity threats, national security events, policy changes, and impact related to FRCS or CYBERSAFE engagements within the scope of the PWS

During the life of this task order the workload in any one task area may grow for a period of time. When a surge requirement is identified by the Government, the surge CLIN will be exercised via written modification. Prior to awarding the modification, the Contracting Officer will provide the Contractor with a written request for surge support specifying the unforeseen, ad hoc, or unplanned increase in workload, the nature of work to be performed, deliverables, and required timeframes.

- The Contractor shall respond to this request in writing within 5 business days with a price quote and Surge Plan, which shall include, approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government.
- Generally, the Contractor shall have the capability to surge contractor staff to meet mission demands in no more than 30 days of the effective date of the modification; however urgent

requirements may demand a surge effort begin within 5 business days.

3.0 The Contractor shall manage workload surges effectively and in a manner that efficiently schedules and applies contractor resources to meet mission requirements and priorities. The Contractor shall meet the surge support requirements without decreasing the current support to, or quality of, any of the other requirements under this task order. Deliverables

Unless otherwise specified by the Navy Client Representative or GSA COR, the Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media/methods established by mutual agreement of the parties.

PWS Ref. No.	DELIVERABLES.	DUE DATE / PLANNED COMPLETION DATE
2.1	Program Management Plan (PMP), inclusive of: ● Communications ● Change Management ● Risk Management	Within 30 calendar days after award Update Annually and as required during performance
2.1	Contractor Quality Control Plan (QCP)	Within 30 calendar days after award Update As Required
2.1	Monthly Status Report (MSR), inclusive of: ● Progress and status of current work ● Financial status reporting	By the 10th of each month, reflecting the activities of the prior month
2.2 2.2.6 2.3.1	Ad Hoc Deliverables, such as but not limited to: ● CYBERSAFE Program Deliverables ● Adversarial Assessment ○ Test Plans ○ Technical Reports ● NAVFAC SETR documentation ● Security Assessment Plans ● Executive Summary for the Security Assessment Reports ● White Papers ● Studies ● Project Plans/ Plan of Objectives and Milestones (POAMS)	As Required, due on date specified when tasking is assigned by Navy designee
2.2.1	NAVFAC SETR Instruction	As Required
6.4	Trip Approval Log	As Required
6.4	Trip Reports	As Required, due not later than 5 business days after completion of trip
6.8	RIP or CTP for ODC purchases	As Required

3.1 Deliverable Media Types

The list below identifies the media types for typical electronic deliverable anticipated under this task order. The Contractor shall submit electronic deliverables in a format compatible with the versions of the specified software in use by the client.

- Text Microsoft Word
- Spreadsheets Microsoft Excel
- Briefings Microsoft PowerPoint
- Drawings Microsoft Visio
- Schedules Microsoft Project

Other file formats (example: .pdf, .pub) may be acceptable as mutually agreed and coordinated with the Government.

3.2 Inspection and Acceptance

Inspection and acceptance of all work performance, reports and other deliverables under this Task Order shall be performed by the Government points of contact designated in PWS 7.1.

3.2.1 Scope of Inspection

Work Products/Deliverables will be surveilled for content, completeness, accuracy and conformance to Task Order requirements.

3.2.2 Basis of Acceptance

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the Contractor's proposal and other terms and conditions of the contract.

a. Reports, documents and narrative type work products/deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.
b. The Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
c. If the Government finds that a draft or final deliverable contains excessive spelling errors, grammatical errors, improper format, or it otherwise does not conform to Navy standards or the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the applicable Navy REPO Client designee.

If a draft is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) work days (unless specified otherwise) from Government receipt of the draft deliverable.

Upon receipt of the Government comments, the Contractor shall have ten (10) work days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

3.3 Non-Conforming Products or Services

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten (10) work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the Contractor will immediately notify the GSA COR of the reason for the delay and provide a proposed corrective action plan within ten (10) work days.

4.0 Key Personnel

The Contractor shall identify skilled, experienced Key Personnel resources that will be essential to the work performed in the PWS. All key personnel shall be identified by name, title/job classification, email/phone, position and company name. The Contractor agrees that the above key personnel shall not be removed from the contract effort. The Contractor shall not replace or move the contractor from the task without at least two weeks' notice to the COR. If any change to the key personnel position becomes necessary (substitutions or additions), the Contractor shall immediately notify the Contracting Officer in writing, accompanied by the resume of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently approved for that category.

- No substitution or replacement of the key personnel shall be approved within the first ninety (90) days after contract award.
- All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change.

The Contractor shall provide a resume to the Government so they can do a comparison of skills and qualifications to those set forth in SOW. Key personnel shall possess the listed experience and expertise for the following functional roles:

4.1 Program Manager – Contract Liaison

The Contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and Contracting Officer's Representative (COR), as applicable. The Contractor PM, located in the contractor's facility (as applicable), shall ultimately be responsible for ensuring that the Contractor's performance meets all government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for contract performance. The PM shall have authority to approve TO modifications in emergent situations. The PM shall also be responsible for, but not limited to, the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the Contractor shall initiate periodic meetings with the COR.

4.2 Lead Validator

The Lead Validator acts as a trusted agent to the FSCA and FSCA Liaison. The Lead Validator should utilize the FSCA Liaison as an advisor to assist in all matters of validation, documentation, vulnerability mitigation, and residual risk determination. The Lead Validator must attain Level 3 (L3) NQV and FQV certification and will manage a team of FQVs sufficient to support the NAVFAC portfolio across all Navy regions. They shall ensure all validators are certified for the level of work they are performing per the Navy SCA guidance, Space and Naval Warfare (SPAWAR) Memorandum, "Navy Qualified Validator (NQV)", October 21, 2018 and the requirements established by NAVFAC CIO Memorandum on August

13, 2020, “Special Requirements for NAVFAC Facility Related Control System Qualified Validator.“ Level 2 (L2) and L3 FQVs may perform independently without supervision. Validations performed by a Level 1 (L1) FQV must be supervised and endorsed by an L3 FQV in addition to the L1 signature. The supervising L3 FQV is solely accountable for a L1 submission.

4.3 Functional Security Control Assessor (FSCA) Liaison

To perform the FSCA function in the most efficient manner, the FSCA may utilize a team of FSCA Liaisons to assist with FSCA responsibilities, where applicable. The FSCA Liaison will act as the FSCA’s direct representative and will interface with the Program Manager/Information System Owner (PM/ISOs), ISSMs, ISSEs, Validators, PSOs, and Functional Authorizing Official (FAO) Cyber Security Analyst (CSAs), as directed. The FSCA Liaison must be a risk assessment SME and provide support and assistance in the Assessment & Authorization (A&A) effort. The FSCA Liaison must also be an FQV.

4.4 Functional Authorizing Official (FAO) Cognizant Security Authority (CSA)

Accountable to provide formal concurrence with the RMF Step 1 Information Categorization for submitted systems and enclaves. Accountable to support the ISSE in the tailoring of Security Controls during RMF Step 2. The Contractor shall provide SME consultative support to the PM and ISSM in creation of the ISCM strategy. This includes responsibilities for providing formal concurrence of Security Control selection and tailoring during RMF Step 2.

The scope of the AO CSA’s responsibilities are to:

- Review the SP, SLCM Strategy, and Security Assessment Report (SAR) Executive Summary submitted by the PM/ISO and SCA and providing recommendations to the AO
- Attend Checkpoints (described in Appendix J) and provide RMF Subject Matter Expert (SME) guidance and initial approval on behalf of the AO
- Ensure authorization requests are supported by sufficient documentation
- Ensure authorization recommendations comply with higher level policy as defined by DoD/Navy policy, instruction, and guidelines in support of the AO authorization decision
- Provide technical analysis of RMF artifacts to inform the authorization decision in support of the AO
- Support the monitoring, tracking and execution of POA&Ms
- Review system level POA&M vulnerabilities and failed security controls and provide recommendations to the AO on PMO/ISO scheduled completion dates to remediate/mitigate open POA&M items as well as recommendations for acceptance of risk

4.5 CYBERSAFE System Security Engineer

The Contractor shall assign a systems security engineer subject matter expert to provide technical oversight ensuring that policies, procedures, and guidance follow cybersecurity principles. This support will ensure the technical aspects of CYBERSAFE activities follow industry standard cybersecurity best practices.

5.0 Security

Work performed under this PWS may be conducted up to the TS SSBI/SCI level; the Contractor may be required to access unclassified and classified information and spaces for meetings and work. The Government will provide a DD254 Department of Defense Contract Security Classification Specification as an attachment to this contract. All contractor personnel supporting and performing on this contract

shall be U.S. citizens and possess at least an interim DoD secret clearance. NAVFAC requires all contractor personnel working on the Federally-controlled facility to have, at a minimum, National Agency Check with Written Inquiries (NACI) or NACI equivalent and favorable completion of a Federal Bureau of Investigation (FBI) fingerprint check.

5.1 Security IT Position Categories

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R (and subsequent revisions), SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or Contracting Officer's representative (COR) in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by NAVFAC Security Office, processed by the OPM, and adjudicated by Department of Defense Consolidated Adjudications Facility (DoD CAF). IT Position Categories are determined based on the following criteria:

5.1.1 IT-I Level (Privileged)

Personnel in this position have:

- Responsibility for the development and administration of Agency computer security programs, including direction and control of risk analysis and/or threat assessment.
- Responsibility for preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

Personnel whose duties meet the criteria for IT-I Position designation shall have a favorably adjudicated Tier 5 (T5) investigation (formerly a Single Scope Background Investigation (SSBI) or SSBI-PR). The T5 is updated a minimum of every 5 years. Personnel assigned to designated IT-I positions shall have a U.S. citizenship unless a waiver request is approved by CNO.

5.1.2 IT-II Level (Limited Privileged)

Personnel in this position have responsibility for planning, design, testing, operation, maintenance, and/or monitoring of a computer system, have privileged access to assets and systems that are tenants on NAVFAC networks and/or similar system constructs, and has work that is technically reviewed by a higher authority at the IT-I Position level to insure the integrity of the system.

Personnel whose duties meet the criteria for an IT-II Position shall have a favorably adjudicated Tier 3 (T3) investigation (formerly National Agency Check with Law and Credit (formerly ANACI/NACLC). Personnel assigned to designated IT-II positions shall have a U.S. citizenship unless a waiver request is approved by CNO.

5.1.3 IT-III Level (Non-privileged)

Personnel in this position support include all other positions (not considered IT-I or IT-II) involved in computer activities. A contractor in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation shall have a favorably adjudicated Tier 1 (T1) investigation National Agency Check with Written Inquiries (formerly NACI).

5.2 Security Investigations

5.2.1 Previously Completed Security Investigations

Previously completed security investigations may be accepted by the Government in lieu of new investigations if determined by the NAVFAC Personnel Security Office to be essentially equivalent in scope to the contract requirements. The length of time elapsed since the previous investigation will also be considered in determining whether a new investigation is warranted, as outlined in SECNAV M-5510.30, Exhibit 5A. To assist the Government in making this determination, the Contractor shall provide the following information to the respective Personnel Security Office immediately upon receipt of the contract. This information shall be provided for each contractor employee who will perform work on a Federally-controlled facility and/or will require access to Federally-controlled information systems:

1. Full name, with middle name, as applicable, with social security number;
2. Citizenship status with date and place of birth;
3. Proof of the individual's favorably adjudicated background investigation or NACI, consisting of identification of the type of investigation performed, date of the favorable adjudication, name of the agency that made the favorable adjudication, and name of the agency that performed the investigation;
4. Company name, address, phone and fax numbers with email address;
5. Location of on-site workstation or phone number if off-site (if known by the time of award); and
6. Delivery order or contract number and expiration date; and name of the Contracting Officer.

The Contracting Officer Representative (COR) will ensure that the Contractor is notified as soon as a determination is made by the assigned or cognizant NAVFAC Personnel Security Office regarding acceptance of the previous investigation and clearance level.

5.2.2 New Security Investigations

If a new investigation is deemed necessary, the Contractor and COR will be notified by the respective NAVFAC Personnel Security Office after appropriate checks in DoD databases have been made.

If the contractor employee requires access to classified information and currently does not have the appropriate clearance level and/or an active security clearance, the Personnel Security Office will relay this information to the contractor and COR for further action. Investigations for contractor employees requiring access to classified information must be initiated by the Contractor Facility Security Officer (FSO).

It is the Contractor's responsibility to ensure that adequate information is provided and that each contractor employee completes the appropriate paperwork, as required either by the COR or the Personnel Security Office, in order to begin the investigation process for the required clearance level.

5.2.3 Security Classification Specification

DD254, Contract Security Classification Specification, delineates the security requirements for this contract. The Contractor is responsible for ensuring that each contractor employee assigned to the position has the appropriate security clearance level. Work performance shall be at the following classification levels: Unclassified, Confidential, Secret, Top Secret/SCI. All personnel assigned to this contract shall have at a minimum, and be able to maintain, a SECRET clearance in accordance with the table below. All personnel security clearances shall be in place prior to individuals reporting for duty at the required Government location.

Key Personnel Requirements	Clearance	Level
Program Manager	Top Secret	SSBI
Lead Validator	Top Secret	SSBI
FSCA Liaison	Top Secret	SSBI
FAO CSA	Top Secret	SSBI
CYBERSAFE System Security Engineer	Top Secret	SSBI

5.3 Cybersecurity Support

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

5.3.1 Cyber IT and Cybersecurity Personnel

The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD

8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

5.3.2 System Access

Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in Para 8.2.2.4(b).

5.3.3 Privileged Access

Contractor personnel with privileged access shall acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

5.3.4 Cyber IT/Cybersecurity Workforce (CSWF) Designation

Contractor personnel shall meet cybersecurity workforce requirements in accordance with DoDD 8140.01 Cyberspace Workforce Management and SECNAV M-5239.2 Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual. All Cyber IT/CSWF personnel must meet and maintain the minimum qualification standards of their assigned Specialty Area, Work Role and proficiency level. Based on the Cyber IT/Cybersecurity function provided by the individual, DON has identified minimum education, training, and industry certification requirements along with proficiency demonstration in the lab or on the job. The contractor shall meet the qualifications required for their functional role based on the following Workforce Element, Specialty Area, Work Role and Proficiency designations.

Key Position	Functional Role	Workforce Element	Specialty Area	Work Role(s)	Proficiency Level
X	Program Manager – Contract Liaison	Cyber IT	Oversee & Govern	IT Project Manager (802)	Advanced
X	Lead Validator	Cyber-security	Securely Provision	Security Control Assessor (612)	Advanced
X	FSCA Liaison	Cyber-security	Securely Provision	Security Control Assessor (612)	Advanced
X	FAO SCA	Cyber-security	Securely Provision	Authorizing Official (611)	Advanced
X	CYBERSAFE System Security Engineer	Cyber IT	Securely Provision	Security Control Assessor (612)	Advanced
	Project Manager	Cyber IT	Oversee & Govern	IT Project Manager (802)	Intermediate
	Data Management Strategy Support	Cyber IT	Operate & Maintain	Database Administrator (421); Data Analyst (422); Knowledge Manager (431)	Intermediate

Key Position	Functional Role	Workforce Element	Specialty Area	Work Role(s)	Proficiency Level
	Enterprise Architecture Support	Cyber IT	Securely Provision	Enterprise Architect (651)	Intermediate
	Automation Support	Cyber IT	Securely Provision	Software Developer (621)	Intermediate
	FRCS Qualified Validators	Cyber-security	Securely Provision	Security Control Assessor (612)	Intermediate
	FSCA Liaison Support	Cyber-security	Securely Provision	Security Control Assessor (612)	Intermediate
	FAO SCA Support	Cyber-security	Securely Provision	Authorizing Official (611)	Intermediate
	CYBERSAFE Support	Cyber IT	Securely Provision	Security Control Assessor (612)	Intermediate

6.0 Administrative Considerations

6.1 Task Order Kick-Off Meeting

The Contractor shall participate in a Kick-Off Meeting with the Government at a time and place scheduled through the GSA Contracting Officer, or designated representative. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved in administration of the Task Order. The meeting will provide the opportunity to discuss contract transition, technical, management, and security considerations; reporting and deliverable submission procedures; travel/ODC approval processes; billing/invoicing procedures; roles/responsibilities, etc. At a minimum, the attendees shall include key representatives of the Contractor, key Government representatives from NAVFAC, and representatives from GSA's Contracting Office.

6.2 Government Points of Contact

GSA Contracting Officer:

Nadya Popil
GSA FAS, Mid-Atlantic Region
The Dow Bldg., 100 S. Independence Mall W., Philadelphia PA 19106-2320
Email: nadya.popil@gsa,gov
Phone: (215) 446-5810

GSA Project Manager / Contracting Officer's Representative (COR):

Eric Fagen
GSA FAS, Mid-Atlantic Region
The Dow Bldg., 100 S. Independence Mall W., Philadelphia PA 19106-2320
Email: eric.fagen@gsa.gov
Phone: 215-446-5831

U.S. Navy Client Representative / Technical Point of Contact (TPOC):

To Be Specified Upon Task Order Award

6.3 Period of Performance

This task order consists of 12-month Base Period with four subsequent 12-months option year. The anticipated periods of performance are as follows:

- Base Year: 15 September 2021 through 14 September 2022
- Option Year 1: 15 September 2022 through 14 September 2023
- Option Year 2: 15 September 2023 through 14 September 2024
- Option Year 3: 15 September 2024 through 14 September 2025
- Option Year 4: 15 September 2025 through 14 September 2026

The Government may extend the term of this task order by written notice to the Contractor within 30 days of the expiration of the existing period of performance provided that a preliminary notice of the Government's intent to extend is provided at least 30 days before the expiration of the task order. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended task order shall be considered to include this option clause. The Government shall have the unilateral right to exercise options periods.

6.4 Hours of Operation

Unless other work hours are coordinated with the Navy Client designee, the Contractor is responsible for conducting work activities, between the core hours of 0800-1700 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings.

6.5 Holidays

Based on mission needs, the contractor may be required to perform services on U.S. holidays. Recognized holidays include:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Juneteenth	Christmas Day
Independence Day	

6.6 Place of Performance

The primary place of performance is Washington DC Metro Area. To promote efficiencies resources may be staffed and or deployed to high Navy Fleet System concentration areas as mission requires.

The Government requires on-site performance at the locations listed within the Performance Work Statement (PWS) on a regular, recurring basis. From time to time, situational telework may be allowed on an ad hoc, case-by-case basis dependent on mission needs and at the unilateral discretion of the Government. Contractor requests for situational telework shall be coordinated in advance by the Contractor PM and submitted for review and approval of the designated NAVFAC TPOC. In the absence of the designated NAVFAC TPOC, the situational telework review and approvals will be handled by the GSA COR or GSA CO. These are the only Government officials with authority to approve telework.

6.7 Travel

Travel to CONUS/OCONUS locations may be required for execution of the contract, including but not limited to the following locations:

- Norfolk, VA
- Guam
- Kings Bay, GA
- San Diego, CA
- Rota, Spain
- Honolulu, HI
- Camp Lemonnier Djibouti (CLDJ), Djibouti
- Port Hueneme, CA

All anticipated travel requests costs shall be reasonable and coordinated with, approved and authorized in writing by the COR prior to commencement of travel. All contract related travel costs shall be in accordance with FAR 31.205-46 Travel Costs, which addresses permissible costs for transportation, lodging, meals, and incidental expenses, and must be accompanied by a Trip Report that details the purpose for travel, work accomplished, identified issues (if any), remaining work to be performed and overall results.

6.7.1 Travel Regulations

The Contractor shall adhere to FAR part 31.205-46 for travel associated with performance on this task order. This shall include all travel requirements associated with temporary duty (TDY) or deployments as required under this task order. Contractor personnel are authorized to invoice travel related costs at the allowance referenced in FAR part 31.205-46.

6.7.2 Travel Authorization Requests

Before undertaking travel to any Government site or any other site in performance of this Task Order, the Contractor shall coordinate with and have travel approved by the COR. The Government shall approve all travel in writing. Travel shall not be considered approved until written approval is received from the COR (Email shall suffice). The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel should be scheduled during normal duty hours, unless mission needs dictate otherwise, subject to COR approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and/or DSSR.

Subject to the review and approval of the COR, post award, the Contractor shall propose and utilize an organized method and format for the tracking and approval process associated with Travel Authorization Requests. The Contractor shall maintain a summary of all its long-distance travel, to include, at a minimum, the information itemized above.

Prior to any long-distance travel, the Contractor shall prepare a Travel Authorization Request for Government review and approval. Travel Authorization Requests shall:

- Include, at a minimum, the number of persons in the party, traveler name(s), destination, duration of trip, purpose, and estimated cost.
- Include a description of the travel, including a statement as to its purpose;

- Be prepared in a legible manner;
- Be summarized by traveler
- Identify the travel request/travel authorization number associated with the travel;
- Be submitted in advance of the travel with sufficient time to permit review and approval.

6.7.3 Foreign Travel

The Contractor shall follow the procedures and process identified in the DOD Foreign Clearance Guide (FCG) when traveling to foreign areas. These procedures include Visa requirements as well as technical expert requirements. Seek clarification from the COR, if needed.

The Contractor shall use the Synchronized Pre-deployment and Operational Tracker (SPOT) application to request Letters of Authorizations (LOA) for all travel to contingency areas. SPOT may also be used to produce LOAs for other overseas locations.

The Contractor shall adhere to requirements of the Defense Base Act (DBA) and the need for insurance while working on U.S. installations/facilities overseas.

Reference:

- FCG: https://www.fcg.pentagon.mil/fcg.cfm.
- SPOT: https://spot.dmdc.mil/privacy.aspx

6.8 Invoicing

The Period of Performance (POP) for each invoice shall be for one calendar month. The contractor shall submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month (for services) or

(2) The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice shall clearly indicate both the current invoice's monthly "burn rate" and the total average monthly "burn rate". The contractor shall submit all required documentation (unless exempted by the contract or order) as follows:

- For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.
- For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Notes:

The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance shall not be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ASSIST or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

GSA
Miscellaneous Receipts
PO Box 979009
St. Louis, MO 63101

Posting Acceptance Documents. Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ASSIST, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance. The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ASSIST, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice. The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number

2. Task Order ACT Number

3. Remittance Address

4. Period of Performance for Billing Period

5. Point of Contact and Phone Number

6. Invoice Amount

7. Skill Level Name and Associated Skill Level Number

8. Actual Hours Worked During the Billing Period

9. Travel Itemized by Individual and Trip (if applicable)

10. Training Itemized by Individual and Purpose (if applicable)

11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice. Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, if necessary.

7.0 Clauses

FAR Clauses:

52.252-2 Clauses Incorporated by Reference

The ALLIANT contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://acquisition.gov/.

52.228-3 Workers' Compensation Insurance (Defense Base Act)

DFARS 252.222-7002, Compliance With Local Labor Laws (Overseas)

DFARS 252.225-7004, Report of Intended Performance Outside the United States and Canada—Submission After Award (OCT 2015)

DFARS 252.225-7006, Quarterly Reporting of Actual Contract Performance Outside the United States (OCT 2010)

DFARS 252.225-7043, Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States (JUN 2015)

DFARS 252.225-7040, Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States (OCT 2015)

For Performance at Camp Lemonnier Djibouti or other locations in the USAFRICOM AOR, FAR part 252.225-7980 deviation applies, to Contractor Personnel Performing in the United States Africa Command Area of Responsibility (DEVIATION 2016-O0008)(JUN 2016), in lieu of the clause at DFARS 252.225-7040, Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States.

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor

rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days

52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

52.216-1 Type of Contract (Apr 1984)

The Government contemplates award of a Hybrid Firm Fixed Price (FFP) / Time & Materials (T&M) contract resulting from this solicitation.

52.237-3 Continuity of Services. (Jan 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to—

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

I The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

8.0 Applicable Documents

Governing documents and applicable regulations, policies, instructions, etc. include but are not limited to the latest edition of the following:

- DoDI 8500.01, Cyber Security Program
- DoDI 8510.01, Risk Management Framework
- DoDD 8140.01 Cyberspace Workforce Management and SECNAV M-5239.2 Cyberspace Information Technology and Cybersecurity Workforce Management
  Reference:
  - https://public.cyber.mil/cw/dcwf/
  - https://www.cool.osd.mil/usn/cswf/index.htm
- SECNAVINST 5239.22 Cybersecurity Safety (CYBERSAFE) Program
- US Navy Risk Management Framework (RMF) Process Guide 3.2
- NAVFAC CIO Memorandum on August 13, 2020, Special Requirements for NAVFAC Facility Related Control System Qualified Validator
- NAVFAC FRCS RMF Business Rules Version 2.0
- NAVFAC CYBERSAFE Grading SOP V 1.0
- NAVFAC CyCx Framework SOP
- Cybersecurity Safety (CYBERSAFE) Technical Warrant Holder

PWS Attachments

- Attachment A - Quality Assurance Surveillance (QASP)
- Attachment B - Performance Requirements Summary (PRS)
- Attachment C - Problem Notification Report (PNR)
- Attachment D - Contract Discrepancy Report (CDR)